NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA-769008

IMAGE ENCRYPTION & AUTHENTICATION USING ORTHOGONAL TRANSFORMATION ON RESIDUAL NUMBER SYSTEM

A project report

Submitted in the partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

In

ELECTRONICS & COMMUNICATION ENGINEERING

By

UMAKANTA SAHU (10609001)

& **In**

ELECTRONICS & INSTRUMENTATION ENGINEERING

By

KALYAN SOURAV DASH (10607008)

Under the guidance of

Prof. G.S. RATH

Department of Electronics & Communication Engineering

National Institute of Technology Rourkela-769008

NATIONAL INSTITUTE OF TECHNOLOGY

ROURKELA-769008

CERTIFICATE

This is to certify that the project entitled "**Image Encryption & Authentication using Orthogonal transformation on Residual Number System**" submitted by Umakanta Sahu (10609001) & Kalyan Sourav Dash (10607008) in partial fulfillments of the requirements for the award of **Bachelor of Technology degree** in Electronics & Communication Engineering at National Institute of Technology, Rourkela, is an authentic work carried out by them under my supervision and guidance.

To the best of my knowledge, the matter embodied in this thesis has not been submitted at any other university or institute for the award of any degree or diploma.

Date:

Prof. G.S. Rath

Department of Electronics & Communication Engg.

National Institute of Technology

Rourkela-769008.

CONTENTS

ABSTRACT

In every communication channel or methodology now-a-days, there is a necessity of secure transmission from sender to the authentic receiver. Therefore a number of data encryption techniques have come up in recent years for different information transfer systems. We are mainly concerned with the types of data, which are represented and interpreted as images. Several classical image encryption approaches like discrete cosine transform or Fourier transform have been proposed and being used. We propose a new method for encrypting images using an orthogonal transformation, namely, Walsh transformation with a key matrix which together fulfill our purpose of cipher. Throughout our operations on image data, we use modular arithmetic so that computations with the resulting residue number system will become efficient. In this paper, we state the algorithm design steps to calculate key matrix which plays the most vital role in any encryption technique. We also show that the total number of possible combinations of key generation is so high for a common brute force or a hacker that virtually it will be impossible to find the authentic key. Also the encryption approach considers image in a divided matrix domain and finally combines all independent cryptographic operations as encryption is a one-to-one mapping. This takes care of the possibility that if any pixel value is ill-stored or wrongly received at the receiver end, which will not affect the decryption process and the final recovered image will differ by a negligible amount. Though this technique is a very simple one, it is very efficient in terms of authenticity, privacy and integrity.

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

Cryptography, defined as *the science and study of secret writing* concerns the ways in which communications and data can be encoded to prevent disclosure of their contents through eavesdropping or message interception, using codes, ciphers and other methods, so that only certain people can see the real message. Cryptography enables us to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, *Cryptanalysis* is the science of analyzing and breaking secure communication. A cryptographic algorithm, known as the *cipher*, is a mathematical function used in the encryption & decryption process. A cryptographic algorithm works in combination with a *key* to encrypt the message. A cryptographic algorithm with all possible keys and protocols is known as a *Cryptosystem*.

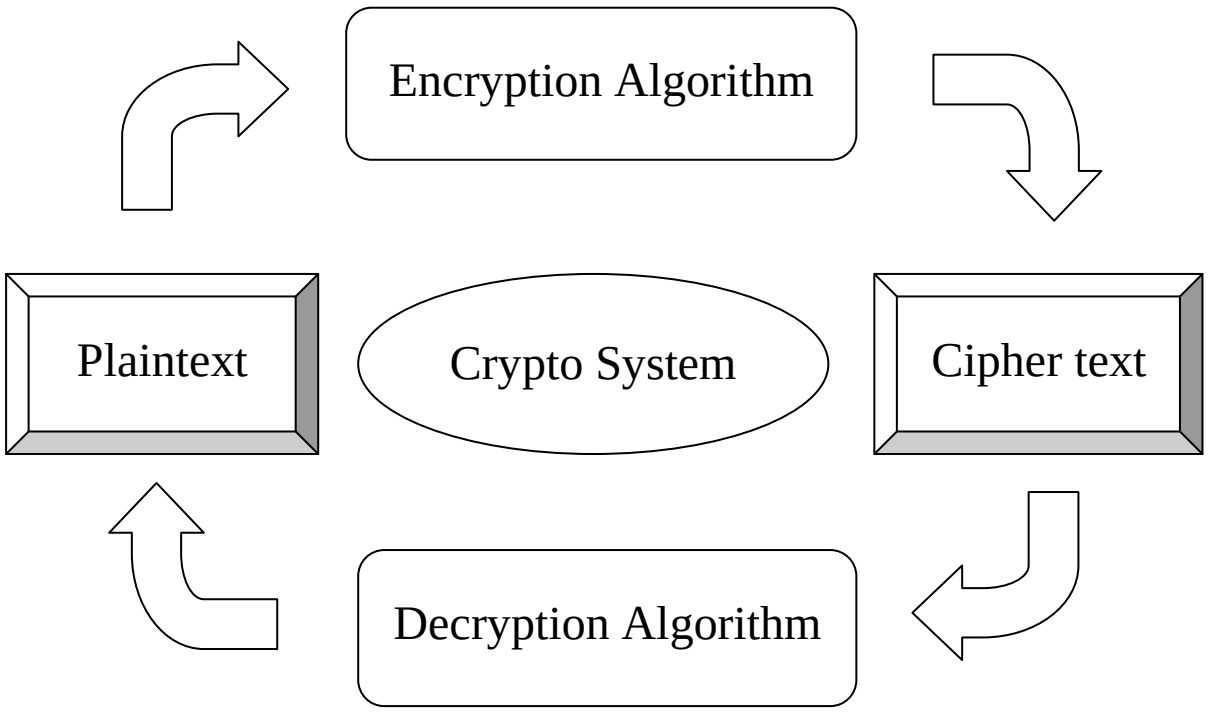

FIGURE.1.1 General Block Diagram of Cryptosystem

Encryption (sometimes called as encipherment) is the process of transforming a piece of information (known as the *plaintext*) using an algorithm (known as the *cipher*) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the *cipher text*. The reverse process of transforming cipher text to plaintext is known as *decryption* (sometimes called as decipherment).

Cryptographic systems are generally classified along three independent dimensions:

1. Type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles. Those are substitution, in which each element in the plain text is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost. Most systems referred to as product systems, involved multiple stages of substitution and transposition.
2. The number of keys used: If sender and receiver use the same key, the system is referred to as symmetric, single key or secret key conventional encryption. If the sender and the receiver each uses a different key the system is referred to as asymmetric, two key, or public-key encryption.
3. The way in which the plaintext is processed: A block cipher processes the input on block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

1.2 CRYPTOGRAPHIC GOALS

There are basically three security goals: confidentiality, integrity and availability. They are described as follows.

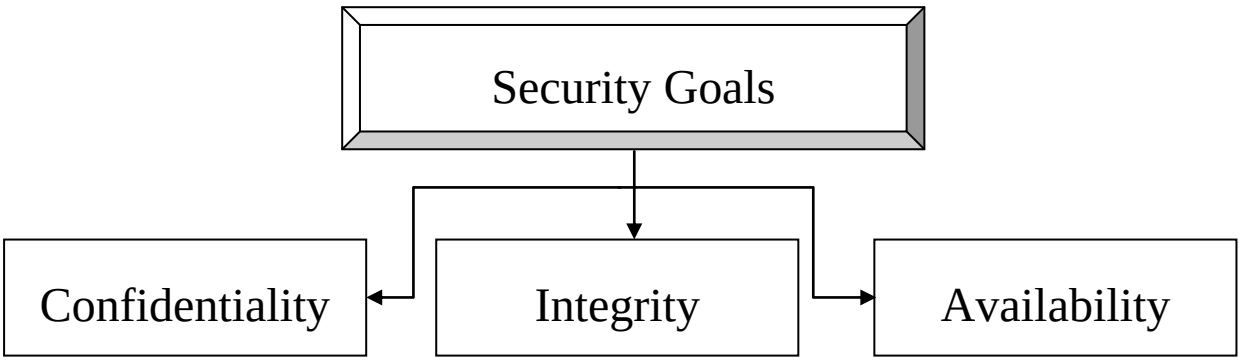

FIGURE 1.2 Taxonomy of Security Goals

1.2.1 CONFIDENTIALITY

Confidentiality is the most common aspect of information security. It is not only applies to the storage of information, but also applies to the transmission of information. That means we need to conceal it during the transmission.

1.2.2 INTEGRITY

Information needs to be changed constantly. Integrity means that these changes need to be done only by authorized entities and through authorized mechanism. Integrity violation is not necessarily the result of a malicious act; an interruption in the system may also create unwanted changes in the information.

1.2.3 AVAILABILITY

The third component of information security is availability. The information created and stored needs to be available to authorized entities. Information is useless if it is not available. Information needs to be changed constantly, which means it must be accessible to authorized entities.

1.3 CRYPTOGRAPHIC SERVICES

The International Telecommunication Union Telecommunication Standardization provides some security services related to the security goals.

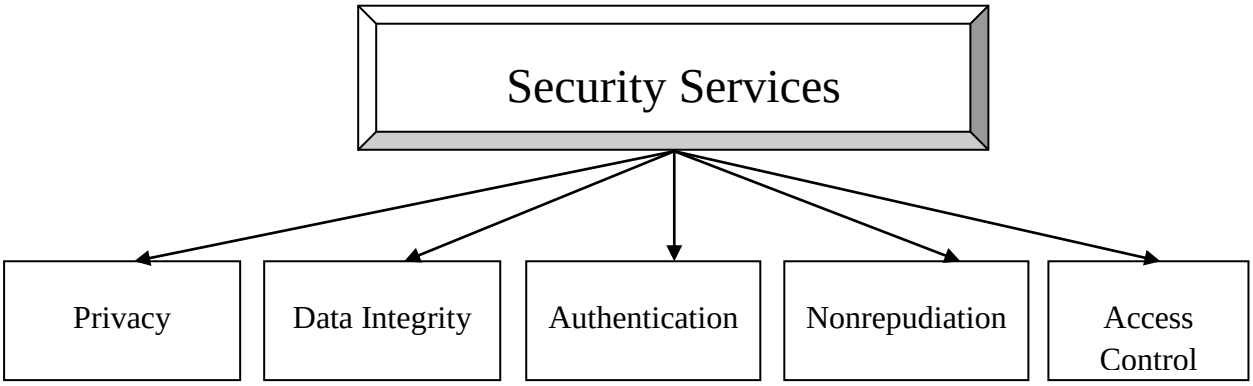

FIGURE 1.3 Taxonomy of security services

1.3.1 PRIVACY

Data confidentiality or privacy is designed to protect data from disclosure attack. This service is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis. That is, it is designed to prevent snooping and traffic analysis attacks. Privacy is typically achieved using *symmetric key ciphers*. These algorithms accept a secret key and then proceed to encrypt the original message and turn it into cipher text.

1.3.2 DATA INTEGRITY

Data integrity is designed to protect data from modification, insertion and deletion. It may protect the whole message or part of a message. Integrity is usually accomplished using cryptographic *one-way hash functions*. These functions accept as an input an arbitrary length message and produce a fixed size *message digest*. The message digest, or *digest* for short, usually ranging in sizes from 160 to 512 bits, is meant to be a representative of the message. That is, given a message and a matching digest, one could presume that outside the possibility of an active attacker the message has been delivered intact.

1.3.3 AUTHENTICATION

Authentication is the property of attributing an identity or representative of the integrity of a message. A classic example would be the wax seal applied to letters. The mark would typically be hard to forge at the time they were being used, and the presence of the unbroken mark would imply the documents were authentic. This service provides the authentication of the party at the other end of

the line. In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment. In connectionless communication, it authenticates the source of the origin of the data.

1.3.4 NONREPUDIATION

Nonrepudiation service protects against the repudiation by either the sender or the receiver of the data. More specifically, it is the inability to refute responsibility. Nonrepudiation is much like the property of authentication in that their implementations often share much of the same primitives. For example, a public key signature can be a

nonrepudiation device if only one specific party has the ability to produce signatures. In Nonrepudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied. In Nonrepudiation with the proof of delivery, the sender of the data can later prove that the data were delivered to the intended recipient.

1.3.5 ACCESS CONTROL

Access control provides protection against unauthorized access to data.

CHAPTER 2

MATHEMATICAL BACKGROUND

2.1 RESIDUAL NUMBER SYSTEM

A *Residual Number System* represents a large integer using a set of smaller integers, so that computation may be performed more efficiently. It relies on *Chinese Remainder Theorem* of modular arithmetic for its operation.

A Residue Number System is defined by a set of N integer constants:

$\{m_1, m_2, m_3 \ldots\ldots m_N\}$, referred to as moduli.

Let M be the Least Common Multiple of all the m_i. Any arbitrary integer X smaller than M can be represented in the defined Residue Number System as a set of N smaller integers as: $\{x_1, x_2, x_3 \ldots x_N\}$ with $x_i = X \bmod m_i$. This relation is called an equivalence relation on integers. An equivalence class comprises of those integers which have the same remainder when divided by m_i. the pairs of integers x_i and X are said to be equivalent or congruent modulo m_i. The set of integers satisfying such congruence relations represents the residue class of X to that modulus.

2.2 CHINESE REMAINDER THEOREM

Let r and s be positive integers which are relatively prime. Let a and b be any two integers. Then there is an integer N such that:

$$N \equiv a \pmod{r} \text{ and } N \equiv b \pmod{s} \tag{2.1}$$

Moreover, N is uniquely determined modulo *r*x*s*. An equivalent statement is that if gcd(r, s) = 1, then every pair of residue classes modulo r and s corresponds to a simple residue class modulo *r*x*s*.

The theorem can be generalized as follows:

Given a set of simultaneous congruences: $x \equiv a_i \pmod{m_i}$, for i = 1 to r and for which m_i are relatively prime. Then the solution to the set of congruences is

$$x \equiv (a_1 \, b_1 \frac{M}{m_1} + \ldots + a_r \, b_r \frac{M}{m_r}) \, (mod \; M) \tag{2.2}$$

Where $M = m_1 m_2 \ldots m_r$, and the b_i are determined form:

$$b_i \frac{M}{m_i} \equiv 1 \ (mod\ m_i) \tag{2.3}$$

2.3 MODULAR MULTIPLICATIVE INVERSE

Two numbers *a* and *b* are multiplicative inverse of eachother if

$$a \times b \equiv 1 \pmod{n} \tag{2.4}$$

Thus the modular multiplicative inverse of *a* modulo *n* is an integer *b* such that :

$$a^{-1} \equiv b \pmod{n} \tag{2.5}$$

The multiplicative inverse of *a* modulo *n* exists *iff a* and n are coprime, i.e,

$$\gcd(a, n) = 1 \tag{2.6}$$

If the modular multiplicative inverse of *a* modulo *n* exists, the operation of division by *a* modulo *n* can be defined as multiplying by the inverse, which is in essence the same concept as division in the field of reals. The modular multiplicative inverse can be found out using various techniques, one of the most efficient being the *Extended Euclidean Algorithm.*

2.4 EXTENDED EUCLIDEAN ALGORITHM

The Extended Euclidean Algorithm can find the multiplicative inverse of *b* in Z_n when *n* and *b* are given and the inverse exists. Let us replace the first integer *a* with *n* (the *modulus*). The algorithm can find *s* and *t* such that :

$$s \times n + b \times t = gcd(n,b) \tag{2.7}$$

However, if the multiplicative inverse of *b* exists, then gcd(*n*,*b*) = 1. So we have now:

$$s \times n + b \times t = 1 \tag{2.8}$$

Now we apply modulo operator to both sides. We will have

$$(s \times n + b \times t) \mod n = 1 \mod n$$

$$=> [(s \times n) \mod n] + [(b \times t) \mod n] = 1 \mod n$$

$$=> 0 + [(b \times t) \mod n] = 1$$

$$=> (b \times t) \mod n = 1 \qquad (2.9)$$

This means that t is the multiplicative inverse of b in Z_n.

CHAPTER 3

MATRIX OPERATIONS ON IMAGE

3.1 IMAGE REPRESENTATION

All images consist of pixels. These pixels may have values in double or byte. An image is represented, for all mathematical purposes, as a matrix. The matrix equivalent of an image of size *N*x*M* pixels is a *N*x*M* matrix, where each pixel corresponds to an element of that matrix. This is a two dimensional image. For a typical colour image like RGB image, the matrix representation will be three dimensional. The additional dimension is for Red or Green or Blue proportions in a two dimensional Grayscale image.

3.2 LINEAR TRANSFORMATION OF MATRIX

Linear transformation can otherwise be visualized as a mapping or a function. For two vector spaces *A* and *B*, a transformation *L* from *A* to *B* is a correspondence that maps to each element *x* in *A* a unique element $y = Lx$ in *B*. Any transformation *L* from a vector space *A* to another vector space *B* is said to be linear, if it satisfies property of additivity, homogeneity and principle of superposition.

Mathematically,

$$L(x_1 + x_2) = Lx_1 + Lx_2 \quad \text{(Additivity)} \tag{3.1}$$

$$L(\alpha x) = \alpha Lx \quad \text{(Homogeneity)} \tag{3.2}$$

$$L(\alpha x_1 + \beta x_2) = \alpha Lx_1 + \beta Lx_2 \quad \text{(Superposition)} \tag{3.3}$$

Symbolically, a linear transformation is represented as:

$$L : A \longrightarrow B : x \longrightarrow Lx \tag{3.4}$$

3.3 EIGENVALUE CALCULATION

Eigenvalues are a special set of scalars associated with a linear system of equations (i.e., a matrix equation) that are sometimes also known as characteristic roots, characteristic values. If the action of a matrix on a nonzero vector changes its magnitude but not its direction, then the vector is called an *eigenvector* of that

matrix. Each eigenvector is multiplied by a scalar, called the *eigenvalue* corresponding to that eigenvector. The eigenspace corresponding to one eigenvalue of a given matrix is the set of all eigenvectors of the matrix with that eigenvalue.

For a square matrix A, if there exists a vector $X \in R \neq 0$ such that

$$AX = \lambda X \tag{3.5}$$

for some scalar λ, then λ is called the eigenvalue and *X* is the eigenvector of *A*.

Let *A* be a *K*x*K* square matrix.

$$\mathrm{A} = \begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{bmatrix} \tag{3.6}$$

With eigenvalue λ, the corresponding eigenvector satisfies:

$$\begin{bmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} \end{bmatrix} \begin{bmatrix} x_1 \\ . \\ . \\ . \\ x_k \end{bmatrix} = \lambda \begin{bmatrix} x_1 \\ . \\ . \\ . \\ x_k \end{bmatrix} \tag{3.7}$$

which is equivalent to the homogeneous system:

$$\begin{bmatrix} a_{11} - \lambda & \cdots & a_{1k} \\ \vdots & \ddots & \vdots \\ a_{k1} & \cdots & a_{kk} - \lambda \end{bmatrix} \begin{bmatrix} x_1 \\ . \\ . \\ . \\ x_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ 0 \end{bmatrix} \tag{3.8}$$

which implies: $(A - \lambda I)\, X = 0$ (3.9)

Where I is the identity matrix.

Solving equation 3.9 we will get all K possible values of λ.

3.4 ORTHOGONAL TRANSFORMATION

Two vectors are *orthogonal* if they are perpendicular. A linear transformation,

$$\mathrm{T} : \mathrm{V} \longrightarrow \mathrm{V}$$

is called an *orthogonal linear transformation* if it preserves the inner product. That is, for all pairs of vectors *x* and *y* in the inner product space *V*,

$$< T_x , T_y > = < x , y > \tag{3.10}$$

This means that *T* preserves the angle between *x* and *y*, and that the lengths of T_x and *x* are equal.

Hadamard transform represents a symmetric orthogonal transformation consisting of number of rows and columns that are powers of 2. It is a generalized class of Fourier transform.

3.4.1 WALSH TRANSFORM

This is a special type of orthogonal transformation formed by rearranging the rows of Hadamard matrix that performs an orthogonal, symmetric, involutional & linear operation on 2^m real numbers.

The Walsh transform W_m is a $2^m \times 2^m$ matrix, known as the *Walsh matrix*, which is a specific square matrix, the entries of which are *+1* or *−1*, and the property that the dot product of any two distinct rows (or columns) is zero.

The Hadamard matrices of dimension 2^k for $k \in N$ are given by the recursive formula:

$$H(2^K) = \begin{bmatrix} H\left(2^{(K-1)}\right) & H\left(2^{(K-1)}\right) \\ H\left(2^{(K-1)}\right) & -H\left(2^{(K-1)}\right) \end{bmatrix} \tag{3.11}$$

For example,

$$H(2^0) = [1]$$

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \text{ and so on.}$$

Now, the Walsh matrix is obtained in such a way that the number of sign changes in a row is in increasing order. So,

$$W_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix};$$

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix};$$

$$W_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix} \text{ and so on.}$$

Observe here the number of sign-changes in a row is in increasing order, i.e. in the first row there is no zero crossing; in the second row, there is one & in the third row, there are two zero crossings etc.

Having all these mathematical backgrounds, we can compute eigenvalues of a symmetric square matrix which will provide us the requisites for the key matrix needed for encryption technique. In the next chapter we shall demonstrate our encryption algorithm using Walsh transformation and that key matrix.

CHAPTER 4

IMAGE ENCRYPTION TECHNIQUE

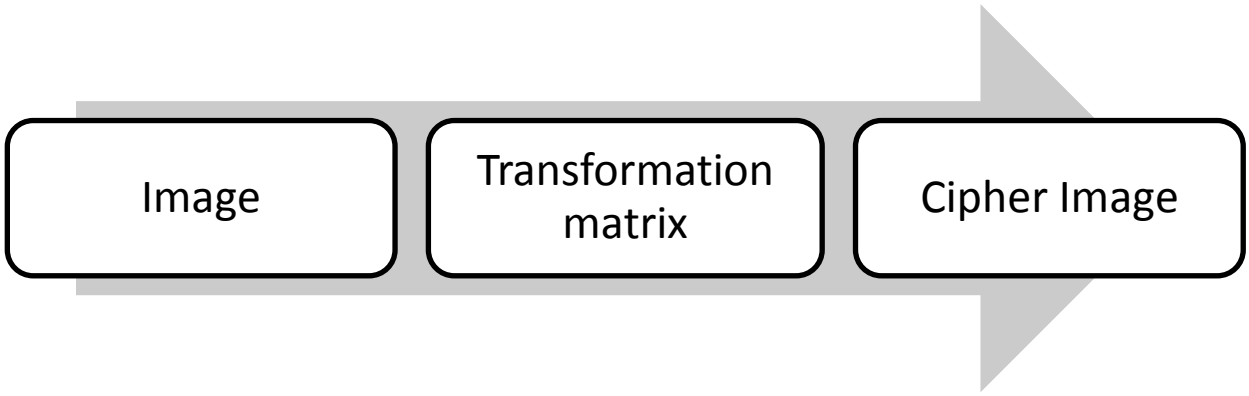

FIGURE 4.1 Flow diagram for encryption technique

4.1 GENERATION OF KEY MATRIX

Key is the essential part of any encryption technique. For encryption of images, the key is a matrix. This key matrix is generated from a particular image which must be available at the receiver end and may be available publicly.

In our proposed encryption technique, first we take a reference image from which the key matrix will be generated. This reference image is available with the party who is the authentic receiver of our image data. The reference image is assumed to be a grayscale image and is represented as a two dimensional matrix. For all encryption purposes, the images are assumed to be having equal number of rows and columns of pixels, the value of which is always in the form 2^m. This is because of the fact that Walsh transformation can only be applied to matrices having 2^m number of rows and columns.

The following steps are involved while calculating the key matrix.

1. The reference image we use is of the size *256* x *256* pixels.
2. Each pixel value is *8*-bit binary, i.e. one byte.
3. We apply modulo *241* operation for our encryption.
4. If pixel value > *241*, it is truncated to *241*.
5. All the *256* rows of the reference matrix are reshaped to *256* x *1* column vectors.
6. The mean vector of all such *256* column vectors is calculated.

7. These column vectors are mean-subtracted and their covariance matrix $\sum$ is computed which will be of dimension *256* x *256*.
8. Now the eigenvalue problem is applied to this covariance matrix to calculate its *256* number of eigenvalues and eigenvectors. Out of these *256* possible eigenvalues, we choose *16* eigenvalues.
9. A diagonal matrix *D* is formed with the chosen eigenvalues as its diagonal entries.
10. Clearly, these eigenvalues are floating point numbers on which we can't directly apply modular operation. Therefore, the matrix *D* is represented as a element-wise division of two matrices *Nr* and *Dr*, where *Nr* and *Dr* represent numerator and denominator values of the elements of matrix *D* respectively.
11. The inverse of the matrix *Dr* is calculated on modulo *241*. This inverse matrix is again element-wise multiplied with the modulo *241* numerator matrix to obtain the required key matrix *K*. Mathematically,

$$K = Dr^{-1}(mod\ 241) .* Nr(mod\ 241) \quad (4.1)$$

This proposed method of key generation is robust and has the obvious advantage that in total, 256^{16} possible combinations of keys can be generated. This is because we are having *256* numbers of eigenvalues to fill *16* diagonal entries. As choosing an eigenvalue is an independent event; so for each diagonal entry we get *256* independent options. Therefore, even if the reference image is available publicly, it will be virtually impossible to obtain the right key out of such huge possible combinations. This directly indicates the efficiency of our encryption technique.

4.2 TRANSFORMATION MATRIX

Till now, we have calculated the key matrix *K*. In our encryption technique, we apply the orthogonal transformation on *16* x *16* matrices. For that reason, we take the Walsh transformation matrix of order *16*, i.e. W_{16} in modulo *241* representation.

The final transformation matrix which will be used as the *cipher*, is given by:

$$W = W_{16}^{T} K W_{16} \tag{4.2}$$

The following steps are involved in the generation of the transformation matrix.

1. Walsh matrix is generated, the entries of which are either *+1* or *-1*.
2. According to the properties of Walsh transform,

$$W_{16}^{T} W_{16} = 16 \text{ x } Identity\ matrix \tag{4.3}$$

   We consider a normalized Walsh matrix so that the right hand side of equation 4.3 contains only the identity matrix. This means an additional term $\frac{1}{4}$ will be multiplied with the original Walsh matrix.

3. As we apply modulo *241* operation upon the Walsh transformation, $+\frac{1}{4}$ is congruent to *181* and $-\frac{1}{4}$ is congruent to *60*.
4. The final transformation matrix *W* is calculated as per equation 4.2.

4.3 IMAGE ENCRYPTION

For encryption of image data the following steps are followed.

1. The image selected as the message is first scaled to *256* x *256* pixels as we are encrypting with this dimension. We can always apply this encryption technique for images having dimension of the order 2^m.
2. Colour images like RGB are multi dimensional. So we convert such images into two dimensional grayscale images.
3. Now modulo *241* operation is operated on this grayscale image.
4. The *256* x *256* pixel image is partitioned and *256* number of *16* x *16* matrices are formed.
5. After dividing the image into *256* number of *16* x *16* matrices, the transformation matrix *W* is multiplied with these *256* number of matrices to form *256* number of cipher image matrices.

6. These *256* number of cipher matrices are then reassembled to form the desired cipher matrix of size *256* x *256*.
7. Finally modulo *241* operation is operated on this cipher matrix. This modulo operated cipher matrix is the final *cipher text* that is to be transmitted.

CHAPTER 5

ENCRYPTION RESULTS

5.1 WALSH TRANSFORMATION MATRIX IN MODULO *241*

181	181	181	181	181	181	181	181	181	181	181	181	181	181	181	181
181	181	181	181	181	181	181	181	60	60	60	60	60	60	60	60
181	181	181	181	60	60	60	60	60	60	60	60	181	181	181	181
181	181	181	181	60	60	60	60	181	181	181	181	60	60	60	60
181	181	60	60	60	60	181	181	181	181	60	60	60	60	181	181
181	181	60	60	60	60	181	181	60	60	181	181	181	181	60	60
181	181	60	60	181	181	60	60	60	60	181	181	60	60	181	181
181	181	60	60	181	181	60	60	181	181	60	60	181	181	60	60
181	60	60	181	181	60	60	181	181	60	60	181	181	60	60	181
181	60	60	181	181	60	60	181	60	181	181	60	60	181	181	60
181	60	60	181	60	181	181	60	60	181	181	60	181	60	60	181
181	60	60	181	60	181	181	60	181	60	60	181	60	181	181	60
181	60	181	60	60	181	60	181	181	60	181	60	60	181	60	181
181	60	181	60	60	181	60	181	60	181	60	181	181	60	181	60
181	60	181	60	181	60	181	60	60	181	60	181	60	181	60	181
181	60	181	60	181	60	181	60	181	60	181	60	181	60	181	60

5.2 KEY MATRIX

53.23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	147.14	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	84.03	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	103.76	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	144.11	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	23.54	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	188.08	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	28.47	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	47.95	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	109.39	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	234.36	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	141.42	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	93.38	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	163.89	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	130.88	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	46.23

5.3 REFERENCE IMAGE FOR KEY GENERATION

FIGURE 5.1

5.4 ENCRYPTION OUTPUTS

5.4.1 IMAGE ‘A’

FIGURE 5.2 Data Image A

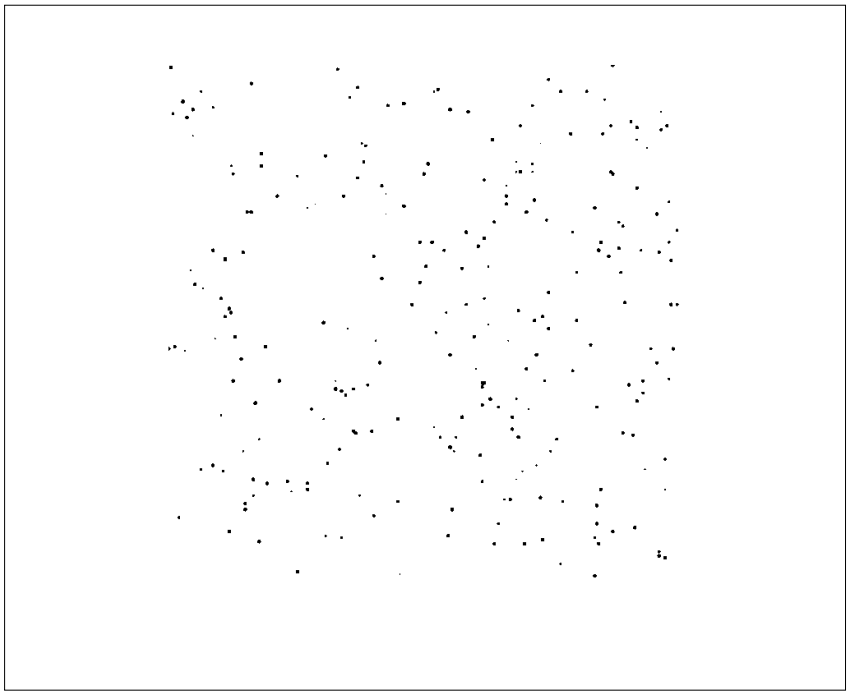

FIGURE 5.3 Encrypted Image A

FIGURE 5.4 Decrypted Image A

5.4.2 IMAGE ‘B’

FIGURE 5.5 Data Image B

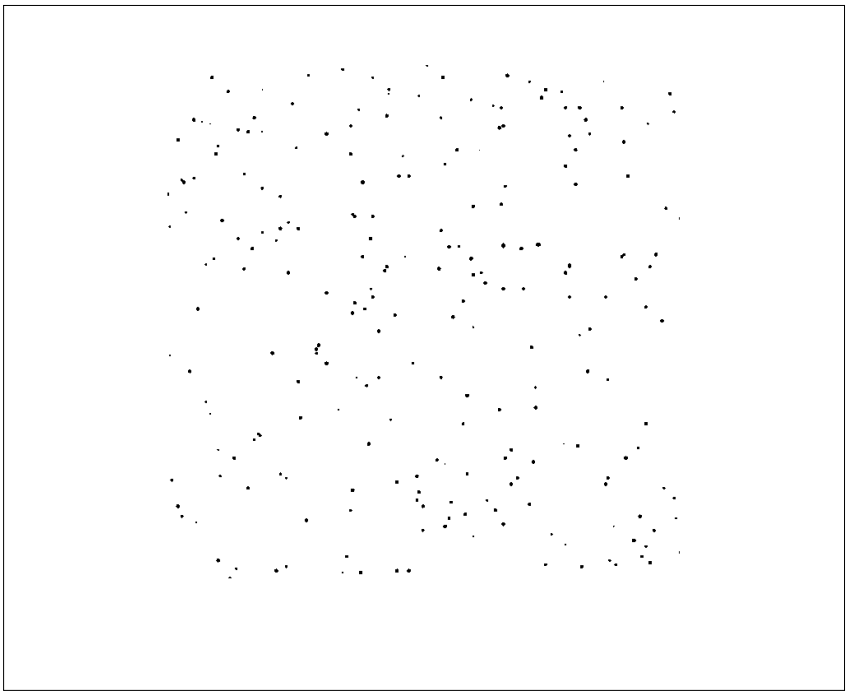

FIGURE 5.6 Encrypted Image B

FIGURE 5.7 Decrypted Image B

5.4.3 IMAGE ‘C’

FIGURE 5.8 Data Image C

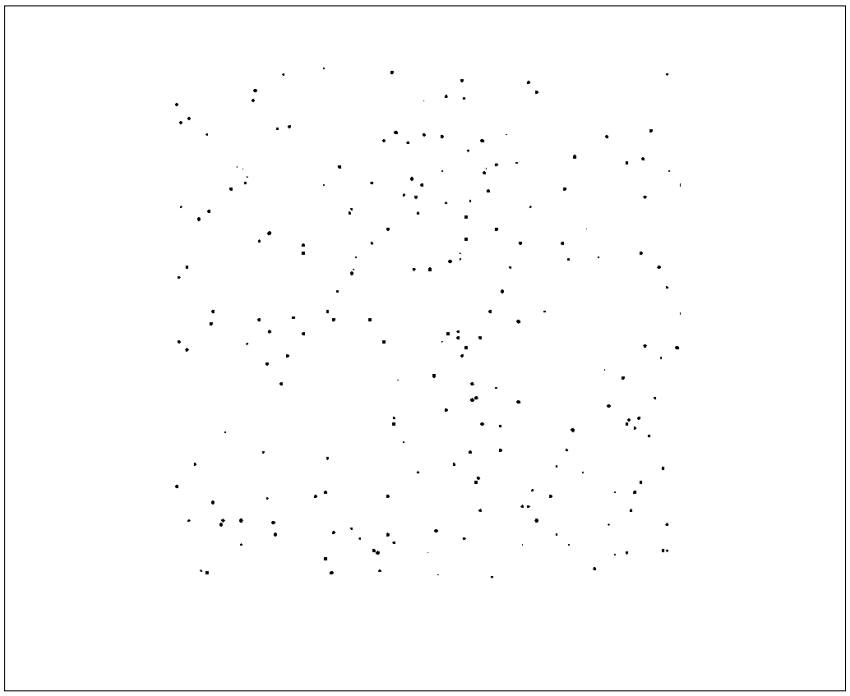

FIGURE 5.9 Encrypted Image C

FIGURE 5.10 Decrypted Image C

CHAPTER 6

CONCLUSION AND FUTURE WORKS

6.1 CONCLUSION

The image encryption method stated in this paper has a great advantage that once encrypted using orthogonal Walsh transformation in modular residual number system, it is very difficult to decrypt. This is because of the fact that the key diagonal matrix we have used for encryption has *16* diagonal entries which are chosen out of *256* available eigenvalues of the covariance matrix of a reference image which means there can be in total 256^{16} possible combinations to look at. So even if the reference image is available as public information, this will be virtually impossible to calculate the diagonal key matrix to decrypt so that only the genuine recipient can decrypt the cipher image successfully. Hence, though this method of image encryption looks simple, it is an efficient approach to deal with.

6.2 FUTURE WORKS

So far in our image encryption technique, we have considered images of size 2^m x 2^m only. This approach can be further extended for other image sizes upon which orthogonal transformation can be implemented. This will increase the flexibility of such encryption method.

Orthogonal transformation on residue number system can also be helpful in data dimension reduction where a very high dimensional data can effectively be reduced to a lower space without much loss of information, thereby eliminating any redundancy and increasing computational efficiency.

References

[1] Cryptography & Network Security by Behrouz A. Forouzan, McGraw-Hill Companies, 2007.

[2] Parhami, Computer Arithmetic, Algorithms and Hardware Design

[3] http://www.mathworks.com/matlabcentral/

[4] Terry Ritter, Walsh-Hadamard Transforms: A Literature Survey.(August 1996)

[5] Yuen, C. 1972. *Remarks on the Ordering of Walsh Functions.* IEEE Transactions on Computers. C-21: 1452.

[6] http://www.nugae.com/encryption/index.htm

[7] W.Stallings; "Cryptography and Network Security" 2nd Edition, Prentice Hall, 1999

[8] Bruce Schneir: Applied Cryptography, 2nd edition, John Wiley & Sons, 1996

[9] Cryptography and Network Security – Behrouz Forouzan

[10] Garfinkel, S.L; "Public Key Cryptography" , Computer, IEEE, Volume: 29, Issue:6, June 1996.

[11] Piper,F "Encryption". Security and Detection, Ecos 97. European Conference.

[12] Flannery, S. and Flannery, D. *In Code: A Mathematical Journey.* London: Profile Books, pp. 123-125, 2000.

[13] Ireland, K. and Rosen, M. "The Chinese Remainder Theorem." §3.4 in *A Classical Introduction to Modern Number Theory, 2nd ed.* New York: Springer-Verlag, pp. 34-38, 1990.

[14] Séroul, R. "The Chinese Remainder Theorem." §2.6 in *Programming for Mathematicians.* Berlin: Springer-Verlag, pp. 12-14, 2000.

[15] Uspensky, J. V. and Heaslet, M. A. *Elementary Number Theory*. New York: McGraw-Hill, pp. 189-191, 1939.

[16] Wagon, S. "The Chinese Remainder Theorem." §8.4 in *Mathematica in Action*. New York: W. H. Freeman, pp. 260-263, 1991.

[17] Apostol, Tom M. (1976), *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, New York-Heidelberg: Springer-Verlag, MR0434929, ISBN 978-0-387-90163-3. See in particular chapters 5 and 6 for a review of basic modular arithmetic.

[18] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Section 31.3: Modular arithmetic, pp. 862–868.

[19] Anthony Gioia, *Number Theory, an Introduction* Reprint (2001) Dover. ISBN 0-486-41449-3

[20] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Pages 859–861 of section 31.2: Greatest common divisor.

[21] Arfken, G. "Eigenvectors, Eigenvalues." §4.7 in *Mathematical Methods for Physicists, 3rd ed.* Orlando, FL: Academic Press, pp. 229-237, 1985.

[22] Hoffman, K. and Kunze, R. "Characteristic Values." §6.2 in *Linear Algebra, 2nd ed.* Englewood Cliffs, NJ: Prentice-Hall, p. 182, 1971.

[23] Kaltofen, E. "Challenges of Symbolic Computation: My Favorite Open Problems." *J. Symb. Comput.* **29**, 891-919, 2000.

[24] Marcus, M. and Minc, H. *Introduction to Linear Algebra*. New York: Dover, p. 145, 1988.

[25] Nash, J. C. "The Algebraic Eigenvalue Problem." Ch. 9 in *Compact Numerical Methods for Computers: Linear Algebra and Function Minimisation, 2nd ed.* Bristol, England: Adam Hilger, pp. 102-118, 1990.

[26] Press, W. H.; Flannery, B. P.; Teukolsky, S. A.; and Vetterling, W. T. "Eigensystems." Ch. 11 in *Numerical Recipes in FORTRAN: The Art of*

Scientific Computing, 2nd ed. Cambridge, England: Cambridge University Press, pp. 449-489, 1992.

[27] "Lincoln Mark VIII speed-sensitive suspension (MPEG video)". Retrieved 2006-09-15.

[28] *Probability, Random Variables and Stochastic Processes*. McGraw-Hill. 2002. pp. 211. ISBN 0-07-366011-6.